What is claimed:

1. A method of improving security processing in a computing network, comprising steps of:

providing a security offload component which performs security handshake processing; and

providing a control function in an operating system kernel for initiating operation of the security handshake processing by the security offload component.

2. The method according to Claim 1, further comprising the step of executing the provided control function, thereby initiating operation of the security handshake processing.

3. The method according to Claim 1, wherein the operating system kernel maintains control over operation of the security handshake processing.

4. The method according to Claim 1, wherein the operating system kernel does not participate in operation of the security handshake processing.

5. The method according to Claim 1, wherein the control function further specifies information to be used by the security offload component during the security handshake processing.

6. The method according to Claim 5, wherein the specified information comprises one or more of: a connection identifier; a security role; one or more security versions supported; and

cipher suites options.

7. The method according to Claim 1, wherein:

the operating system kernel does not participate in operation of the security handshake processing;

the control function further specifies information to be used by the security offload component during the security handshake processing; and

the specified information comprises one or more of: a connection identifier; a security role; one or more security versions supported; cipher suites options; and security certificate key ring information.

8. The method according to Claim 7, wherein the specified information further comprises segment size and sequence number information to be used when transmitting messages of the security handshake processing.

9. The method according to Claim 7, further comprising the step of sending a completion response from the security offload component to the operating system kernel upon completion of the security handshake processing, wherein the completion response conveys information for use by the operating system kernel in carrying out secure communications on a secure session which results from the security handshake processing.

10. The method according to Claim 9, wherein the conveyed information comprises one or

more of: an identifier of the secure session; one or more session keys; a current sequence number for messages of the secure session; a cipher suite to be used for the secure session; a protocol version to be used for the secure session; and a digital certificate or other security credentials.

11. The method according to Claim 1, wherein the operating system kernel maintains control over operation of the security handshake processing, and wherein the operating system kernel provides one or more message segments to the security offload component for use by the security offload component in completing steps of the security handshake processing.

12. The method according to Claim 11, wherein a selected one of the one or more message segments directs the security offload component in a client device to perform random number generation when creating an initial handshake message to transmit to a server device.

13. The method according to Claim 12, wherein the initial handshake message is a Client Hello message.

14. The method according to Claim 11, wherein a selected one of the one or more message segments directs the security offload component in a server device to perform random number generation when creating an initial handshake response message to transmit to a client device.

15. The method according to Claim 14, wherein the initial handshake response message is a Server Hello message.

16. The method according to Claim 11, wherein a selected one of the one or more message segments directs the security offload component in a server device to decode a client security certificate which has been transmitted from a client device.

17. The method according to Claim 11, wherein a selected one of the one or more message segments directs the security offload component in a client device to decode a server security certificate which has been transmitted from a server device.

18. The method according to Claim 11, wherein a selected one of the one or more message segments directs the security offload component in a client device to generate and encrypt a pre-master security secret to be transmitted to a server device.

19. The method according to Claim 18, wherein the encryption of the pre-master security secret uses a public key of the server device.

20. The method according to Claim 11, wherein a selected one of the one or more message segments directs the security offload component in a server device to decrypt a pre-master security secret transmitted from a client device.

21. The method according to Claim 20, wherein the decryption of the pre-master security secret uses a private key of the server device.

22. The method according to Claim 11, wherein a selected one of the one or more message segments directs the security offload component in a client device to compute one or more master security secrets and one or more session cryptography keys to be transmitted to a server device.

23. The method according to Claim 11, wherein a selected one of the one or more message segments directs the security offload component in a server device to compute one or more master security secrets and one or more session cryptography keys to be transmitted to a client device.

24. The method according to Claim 11, wherein a selected one of the one or more message segments directs the security offload component in a client device to digitally sign a message to be transmitted to a server device.

25. The method according to Claim 11, wherein a selected one of the one or more message segments directs the security offload component in a server device to validate a digital signature of a message received from a client device.

26. The method according to Claim 11, wherein a selected one of the one or more message segments directs the security offload component in a client device to compute a message authentication code ("MAC") of the security handshake, wherein the computed MAC is to be transmitted to a server device.

27. The method according to Claim 11, wherein a selected one of the one or more message segments directs the security offload component in a server device to compute a message authentication code ("MAC") of the security handshake, wherein the computed MAC is to be transmitted to a client device.

28. The method according to Claim 11, wherein a selected one of the one or more message segments directs the security offload component in a client device to validate a message authentication code ("MAC") of the security handshake, wherein the MAC was transmitted from a server device.

29. The method according to Claim 11, wherein a selected one of the one or more message segments directs the security offload component in a server device to validate a message authentication code ("MAC") of the security handshake, wherein the MAC was transmitted from a client device.

30. The method according to Claim 11, further comprising the step of sending a completion response from the security offload component to the operating system kernel upon completion of the security handshake processing, wherein the completion response conveys information for use by the operating system kernel in carrying out secure communications on a secure session which results from the security handshake processing.

31. The method according to Claim 30, wherein the conveyed information comprises one or more of: an identifier of the secure session; one or more session keys; a current sequence number for messages of the secure session; a cipher suite to be used for the secure session; a protocol version to be used for the secure session; and a digital certificate or other security credentials.

32. The method according to Claim 31, wherein the conveyed information further comprises a current transmission control sequence number for transmitting messages of the secure session.

33. A method of improving security processing in a computing network, comprising steps of:

providing a security offload component which performs security session establishment and control processing; and

providing a control function in an operating system kernel for initiating operation of the security establishment and control processing by the security offload component.

34. A system for improving security processing in a computing network, comprising:

means for performing security session establishment and control processing in a security offload component; and

means for executing a control function in an operating system kernel, thereby initiating operation of the means for performing security establishment and control processing by the security offload component. .

35. A computer program product for improving security processing in a computing network,

the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code means for performing security session establishment and control processing in a security offload component; and

computer-readable program code means for executing a control function in an operating system kernel, thereby initiating operation of the computer-readable program code means for performing security establishment and control processing by the security offload component.